| | | | |
|---|---|---|---|
| GUAM WATERWORKS AUTHORITY | **STANDARD OPERATING PROCEDURE** | No. | SOP-1200-IT-003 |
| | **Information Technology and Data Center Security** | Effective Date | 12/10/2010 |
| | | Final Approver | Miguel C. Bordallo, P.E.<br>General Manager |
| | | Revision Letter | A |

## 1.0 Purpose

Guam Power Authority (GPA) and Guam Waterworks Authority's (GWA or Authority) Information Technology (IT) departments share the same office/work area and Data Center. The Data Center houses both Authorities' Servers, Disk Arrays, Core Networking Equipment, Storage, and other backend systems and devices, whereas the IT Office work areas contains confidential, restricted and non-public data and information that must be safe guarded. The IT Office work area and the Data Center are classified as controlled and restricted areas.

The purpose of this policy is to help ensure that the Information Technology departments, Data Centers, and equipment hosted therein, remains secure by having in place guidelines and procedures to restrict access to authorized personnel only.

## 2.0 Scope

The Information Technology and Data Center Security Policy seeks to follow best practice regarding physical security for the Data Centers and Intermediate Distribution Facilities (IDF) supporting both GPA and GWA equipment. The objective of this Standard Operating Procedure (SOP) is to minimize security risks and help ensure the safety of IT staff and all the equipment hosted in the Data Center and IDF by monitoring the physical access to GPWA Data Centers.

This policy is intended to create a governance structure and guidelines for the Information Technology and Data Center Security. It applies to all users. This policy represents the commitment of the Authority to protect its systems and information from intentional or unintentional acts that may negatively impact system security.

## 3.0 Policy

Access to the Data Center shall be controlled, logged, and restricted to appropriate personnel as defined and required by their roles and responsibilities. Access to the IT department work area is permitted for specific tasks.

## 4.0 Definitions

4.1. **<u>Access Control System Badge (ACS Badge)</u>** – An electronic key that is programmed to provide entry into specific doors and/or buildings at specific times. Also see the following:

4.1.1. Guam Waterworks Authority SOP-GM-120, Physical Security and Access Control System

4.1.2. Guam Power Authority Policy AP-083 Physical Security and Access Control System

4.1.3. Memo dated May 21, 2019, Changes in the Programming of ACS Badge Access for more information about ACS Badge issuance and use policy

4.2. **Data Center** – A secured, environmentally controlled facility hosting Authority servers and storage arrays that store, transmit or process data.

4.3. **Data Center Administrator (DCA)** – Designated GPA and GWA IT employees assigned to manage Data Center and its access. DCA is generally the Network Administrator unless otherwise designated by Chief Information Technology Officer (CITO) or Information Technology Manger (ITM).

4.4. **Devices** – Server, Desktop Computer, laptop, tablet, thin client, phone instrument including smart phone, removable storage and any other hardware that a User operates to interact with GWA applications and data. This Standard Operating Procedure (SOP) does not cover peripheral devices such as keyboard and mouse.

4.5. **IT Department** - Personnel assigned to the IT departments.

4.6. **Intermediate Distribution Facility (IDF)** – Also known as communication closets or comm rooms.

4.7. **Users** – Are all employees, board members, contractors, consultants, vendors, temporary workers, volunteers, third party, and other persons in a position to know or access information or devices on GWA network.

4.8. **Visitors** – All Non-IT employees, vendors, contractors, sub-contractors, temporary workers, and ALL others, who, through contractual arrangement and prior approvals, require access to the IT Department and must be escorted into the Data Center.

## 5.0 Roles and Responsibilities

| | | |
|---|---|---|
| 5.1. | General Manager | Approve all changes in this SOP.<br>Manage and control the overall operations and all properties of GWA. |
| 5.2. | Assistant General Manager for Administration and Support | Oversee development, revision and implementation of this SOP as the Policy Owner.<br>Represent IT Department in the SOP Committee. |
| 5.3. | Information Technology Manager (ITM) and IT Department | Provide oversight and guidance in complying with GWA IT cybersecurity policy (effective date 07/28/2017).<br>Implement IT Standard Operating Procedures and monitor GWA IT systems to ensure compliance thereto. |

| | | |
|---|---|---|
| | | Monitor GWA systems to ensure compliance with regulatory requirements and standards.<br>ITM Represent IT Department in the SOP Subcommittee. |
| 5.4. | Information Security Administrator | Monitor and ensure compliance with this SOP.<br>Provide training for new employees and annual refresher training for existing employees about the requirements of this SOP. |
| 5.5. | Human Resources | Present each new employee, contractor or vendor with the existing GWA IT policies and procedures, upon the first day of commencing work with GWA. |
| 5.6. | Managers and Supervisors | Ensure that users are informed of appropriate use of GWA equipment and information technology resources through cybersecurity training and compliance with SOP-1200-IT-004, Acceptable Use of Information Technology (Computer, Software, License, E-mail, Internet, and Standards of Conduct). |
| 5.7. | Users | To know this SOP and to conduct their activities accordingly. When GWA computer and system users are confronted by a situation not covered by this SOP or they do not clearly apply to a situation, users are encouraged to clarify with their respective supervisor or the IT Department. |

## 6.0 Procedure Description

### 6.1. Physical and Environmental Security

Security perimeters shall be defined to protect areas that contain confidential or sensitive data, information and/or information systems. Procedures will be defined and enforced to ensure the areas are secured and protected by appropriate access controls, where only authorized personnel are allowed.

6.1.1. Entrance into the Data Center or IDF shall be kept locked at all times with access restricted to IT Department and Visitors when escorted.

6.1.2. IT Department and Visitors must use an ACS badge prior to entering the Data Center or IDF.

6.1.3. Physical Keys must only be used when the access control system is not working.

6.1.4. In the event of equipment delivery, the authorized individual who opened the door is responsible for monitoring the door until it is closed to ensure security and safety and that no unauthorized personnel remains in the vicinity.

6.1.5. All personnel are required to ensure systems are secured and not left open to access by intruders or unauthorized personnel.

6.1.6. All Visitors entering the Data Center or IDF must sign in and out of the IT department Visitors Log Book, documenting their Name, Company, and purpose of visit. Log book shall be maintained by DCA and may be audited by the Internal Audit department unannounced and/or as necessary.

6.1.7. All Visitors granted access into the Data Center or IDF must be escorted at all times by an authorized IT department personnel or an authorized sponsor. Authorized sponsors are limited to the IT department and Power System Control Center (PSCC) SCADA support personnel.

6.1.8. All IT Department and Visitors installing, modifying or exchanging devices, switches, ups or other equipment in the Data Center of IDF must document the activity in the Log Book within the Data Center or IDF to include their Name, Company, and purpose of visit. Log book shall be maintained by DCA and may be audited by the Internal Audit department unannounced and/or as necessary.

6.1.9. All hand-carry containers, boxes, bags, laptops, purses, backpacks, or equipment carried into or out of the Data Center or IDF are subject to inspection by IT Departments.

6.1.10. All external devices brought into the Data Center are subject to inspection and must be approved for use within the Data Center by the CITO, ITM or DCA.

6.1.11. Authorizations will be verified on a quarterly basis (see section 8.0).

6.1.12. Testing on Fire and Protection systems shall be performed annually.

### 6.2. Policy on Access into the Data Center

Entrances into the Data Center shall be by means of Access Control and will be recorded in the Visitors' Log Book. Data Center Entrance door shall remain locked at all times.

6.2.1. Accesses granted to IT Department and Visitors shall not be shared.

6.2.2. General Entry into a Data Center or IDF. "Piggybacking" or "tailgating" is prohibited. Each person entering must use an ACS Badge or be escorted by an IT employee, except for health or safety emergencies.

6.2.3. Should another department's equipment be hosted in the Data Center, access will be granted to the assigned support staff within that department. The CITO, ITM, DCA or designee and the department Manager or designee of the hosted system are responsible for authorizing access to pertinent staff and shall maintain a log of individuals who have been granted access. Individuals without proper authorization will be considered a visitor and shall be escorted by an authorized IT personnel. Access granted to the assigned support staff shall not be shared.

6.2.4. Visitors who require access into the Data Center to perform maintenance or similar work relating to equipment hosted in the Data Center must arrange and be approved by the CITO, ITM or DCA in advance.

6.2.5. All Visitors shall be accompanied and escorted by their authorized sponsor. All visitors must be aware of and abide by existing security policies, and safety rules for visitors entering a work or private area. This includes obtaining and wearing of a visitor's badge (at all times) as issued by the Human Resource department, and signing the Log book to include sign-in when entering, date, time, and purpose of visit.

6.2.6. Access into the Data Center is restricted to authorized sponsors and employees, vetted vendors, external auditors, and government regulatory officials.

6.2.7. Equipment installations, removals, and changes within the Data Center systems must have prior written approval by the CITO, ITM or DCA with an approved Scope of Work (SoW). Entry will be denied to authorized staff or visitors who intend to install, remove, or change equipment without presentation of approved SoW documentation.

### 6.3. Data Center and IDF Etiquette

In order to maintain a clean and safe environment and not obstruct work performed in the Data Center or IDF, all individuals working within the Data Center room must adhere to the following rules of etiquette:

6.3.1. Exterior Data Center and IDF doors shall never be propped open. These access doors are monitored and alarmed.

6.3.2. Under no circumstances shall food or beverage of any type and/or any kind be brought into the Data Center or IDF.

6.3.3. All work areas must be kept clean and free of debris. Upon completion of any work in the room, authorized staff performing the work must ensure that the area is clean before leaving the work area.

6.3.4. All packing materials must be removed from newly delivered computer equipment/components in a designated staging area before being moved into the Data Center or IDF. This includes cardboard, paper wraps, peanuts, plastic, wood, and other such materials used to secure the equipment during shipment.

6.3.5. Avoid obstructing aisles, walkways, or leaving floor tiles unsettled minimizing safety hazards in the Data Center or IDF.

6.3.6. "Un-racked" equipment, i.e. operating equipment outside of cabinets or racks, is strictly prohibited.

6.3.7. All rack enclosures must be kept neat and free of manuals, cables, etc. Doors to each rack must be locked upon completion of work.

6.3.8. The tops of cabinets or any other area of the data center may not be used for physical storage.

6.3.9. Cables shall not be strung outside of rack enclosures. Cabling between rack enclosures of adjacent racks are accepted provided sufficient pass-through chassis are in place. Cable trays must be used.

6.3.10. No cleaning fluids or water are allowed within the Data Center and IDF.

6.3.11. No cutting of materials (pipes, floor tiles, etc.) shall be performed inside the Data Center or IDF.

6.3.12. Photos are not allowed to be taken in the Data Center or IDF.

6.3.13. Only authorized personnel shall be given access to racks that contain equipment for which they are responsible.

6.3.14. Decommissioned equipment shall be removed immediately upon written approval by the CITO, ITM or DCA.

6.3.15. All hard drives must be sanitized and disposed of properly after removal from any and all systems by authorized IT Department.

6.3.16. All equipment hosted within the Data Center or IDF must be inventoried annually as physical assets by the GPA or GWA IT departments.

6.3.17. Health and Safety Rules are applicable when working within the Data Center or IDF. Authorized personnel are to be cognizant of their surroundings and consider potential health hazards. It is recommended for authorized personnel to always be aware of electrical configuration for safety, wear pertinent safety gear if necessary, and use proper lifting and handling protocol.

### 6.4. **Audit Procedures**

6.4.1. The DCA will send a list of authorized staff and authorized vendors to the CITO or ITM on a quarterly basis (October, January, April and July) for review and concurrence.

6.4.2. CITO or ITM will review and update the list of authorized staff/vendors and return it to the DCA within two weeks.

6.4.3. Failure to return access audits will result in revocation of access privileges for previously authorized Visitors until such time as the audit is returned.

### 6.5. Standard of Conduct

Standards of ethical conduct and appropriate behavior apply to the use of all GPWA information technology resources and entry into the IT & Data Centers. Authority Data Centers must not be misused as follows:

6.5.1. Violations of Data Center rules of etiquette (see section 7.0).

6.5.2. Mishandling or abuse of GPA or GWA equipment and/or property.

6.5.3. Allowing any visitor unescorted entrance to Data Center.

### 6.6. Policy Enforcement & Compliance

Users are expected to report suspected violations of this policy to the IT department, their supervisor or manager, or the Internal Audit department. Where guidance or interpretation of this policy is needed, users are advised to discuss the situation with their supervisor or IT department staff for proper guidance and direction.

Violation of this policy may result in limiting or revoking access into the IT & Data Centers in addition to other disciplinary action determined to be appropriate by management.

6.6.1. Compliance Measurement - The IT department team will verify compliance to this policy through various methods, including but not limited to, IT monitoring tools and reports and reports of abuse or noncompliance. Employees and users are expected to report suspected violations of this policy to the IT department, their supervisor or manager, or the Internal Audit department. Potential, detected, or reported deviations from this policy may be documented in the respective GPWA ***IT Incident Reporting Form*** (see Attachment 1).

6.6.2. Exceptions - GPA or GWA IT departments acknowledge that under rare circumstances certain users may ne

6.6.3. ed to employ systems that are not compliant with the policies. Exception to the Data Center Security Policies and Procedures may be granted by the CITO, ITM or designee if it becomes necessary to provide emergency access to medical, fire and/or police and/or Federal Officials, etc.

6.6.4. Non-Compliance - Any user found to have violated this policy may be subject to progressive disciplinary action ranging from a verbal warning to dismissal as outlined in the Authority's Codes of Conduct. The severity and/or adverse effect(s) of the infraction(s) on GPA or GWA's operation and security will be considered. If offense is found to be willful, users may be held personally liable for damages caused by any violations of this policy.

## 7.0 Document Approvals

| Role | Position | Name of Approver | Approval Signature | Date Approved |
|---|---|---|---|---|
| Author | | GPWA IT departments | Approval on File | 12/03/2019 |
| Owner | Assistant General Manager for Administration and Support | Christopher M. Budasi | Approval on File | 12/03/2019 |
| Final Approver | General Manager | Miguel C. Bordallo, P.E. | Page 1 | 12/10/2019 |

## 8.0 Records of Revisions

All suggestions for improvement shall be directed to the Subject Expert indicated below. The subject expert will consider input received, develop recommendations on how to address the suggestions, and obtain authorization to make the recommended changes. Updates, revisions, corrections and waivers to this SOP shall be made in writing and be approved by the GM.

Policy Owner: Assistant General Manager for Administration and Support

Authorization: General Manager

| Effective Date | Revision Letter | Document Author | Description of Change |
|---|---|---|---|
| 12/10/2019 | A | GPWA IT departments | Initial Release of Policy/Procedure |

## 9.0 References

1. GPA Policy IT Data Center Security Policy
2. Notes provided by AGM for Administration & Support
3. CCU Resolution on Cybersecurity Policies and Procedures:
   - GPA Resolution No. 2018-14
   - GWA Resolution No. 38-FY2018

**Attachment 1: IT Incident Reporting Form**

GUAM WATERWORKS AUTHORITY
"Better Water. Better Lives."
Gloria B. Nelson Public Service Building
688 Route 15, Mangilao, Guam 96913

# IT Incident Reporting Form

**Instructions: This form is to be completed as soon as possible following the detection or reporting of an Information Technology (IT) security incident. All items completed should be based on information that is currently available. This form may be updated and modified if necessary.**

| | |
|---|---|
| **1. Contact Information for this Incident** | |
| Name: | |
| Title: | |
| Division: | |
| Work Phone: | |
| Mobile Phone: | |
| Email address: | |

**2. Incident Description.**

Provide a brief description: ***(Attach separate sheet or additional documentation if needed)***

**3. Impact / Potential Impact** Check all of the following that apply to this incident.

□ Loss / Compromise of Data
□ Damage to Systems
□ System Downtime
□ Financial Loss
□ Other Organizations' Systems Affected
□ Damage to the Integrity or Delivery of Critical Goods, Services or Information
□ Violation of legislation / regulation
□ Unknown at this time

Provide a brief description: ***(Attach separate sheet or additional documentation if needed)***

## Attachment 1: IT Incident Reporting Form Cont.

**4. Sensitivity of Data/Information Involved** Check all of the following that apply to this incident.

| **Sensitivity of Data** | |
|---|---|
| **Category** | **Example** |
| **Public** | This information has been specifically approved for public release by Federal/Guam law or Guam Waterworks Authority (GWA) rules, regulations or policy. Unauthorized disclosure of this information will not cause problems for GWA, its clients, or its business partners. Examples are brochures and material posted to Guam Waterworks Authority web pages. |
| **Internal Use Only** | This information is intended for use within the Guam Waterworks Authority or with Government of Guam branches and agencies, and in some cases with business partners. Unauthorized disclosure of this information to outsiders may be against laws and regulations, or may cause problems for the GWA, its customers, or its business partners. Examples are business process forms, payroll information, draft documents and physical security plans/documents. |
| **Restricted/Confidential (Privacy Violation)** | This information is private or otherwise sensitive in nature and must be restricted to those with a legitimate business need for access. Unauthorized disclosure of this information to people without a business need for access may be against laws and regulations, or may cause significant problems for the GWA, its customers, or its business partners. Decisions about the provision of access to this information must be cleared through the information owner. Examples are retirement contribution payments, worker performance evaluation records, legal information protected by attorney-client privilege, customer information and employee personal information such as social security and direct deposit bank account numbers. |
| **Unknown/Other** | Describe in the space provided |

| | |
|---|---|
| □ Public<br>□ Internal Use Only | □ Restricted / Confidential (Privacy violation)<br>□ Unknown / Other – please describe: |

Provide a brief description of data that was compromised: ***(Attach documentation if needed)***

**5. Who Else Has Been Notified?**

Provide Person and Title:

**6. What Steps Have Been Taken So Far?** Check all of the following that apply to this incident.

| | |
|---|---|
| □ No action taken<br>□ System Disconnected from network<br>□ Updated virus definitions & scanned system | □ Restored backup from tape<br>□ Log files examined (saved & secured)<br>□ Other – please describe: |

## Attachment 1: IT Incident Reporting Form Cont.

| | |
|---|---|
| Provide a brief description: ***(Attach separate sheet or additional documentation if needed)*** | |
| **7. Incident Details** | |
| Date and Time the Incident was discovered: | |
| Has the incident been resolved? | |
| Physical location of affected system(s): | |
| Number of sites affected by the incident: | |
| Approximate number of systems affected by the incident: | |
| Approximate number of users affected by the incident: | |
| Are non-Guam Waterworks Authority systems, such a business partners, affected by the incident? (Y or N – if Yes, please describe) | |
| Please provide any additional information that you feel is important but has not been provided elsewhere on this form. | |

**Please submit this completed form to:**
mapuron@guamwaterworks.org
Telephone# 1 671 300-6833

***Investigated by:*** ____________________ Title: IT Manager Date: __________

***Concurred by:*** ____________________ Title: AGM-A&S Date: __________

cc: AGM
Division Manager
For any incidents resulting in adverse action or business system interruptions greater than one (1) hour, General Manager, Human Resources and Internal Audit to be copied.